Patient Command, Inc.
McLean, Virginia 22101

June 4, 2007

Via Electronic Mail to cps-wkg@hsrnet.com

Confidentiality, Privacy and Security Workgroup
American Health Information Community
c/o Office of the National Coordinator
330 C Street, SW, Suite 4090
Washington, DC 20201

Dear Members of the CPS Workgroup:

Patient Command, Inc. submits these comments in response to the May 23, 2007 notice to the Health-IT Listserv. The notice solicits comments on whether the CPS Workgroup should continue to use its current working hypothesis regarding privacy and security. That hypothesis, to paraphrase, is that the privacy and security requirements of HIPAA (the Health Insurance Portability and Accountability Act of 1996), or equivalent requirements, should apply to participants (other than consumers) in electronic networks designed to exchange consumers' health information.

Patient Command believes the answer to this question is "no."

Background: Patient Command and the Health Record Bank Model

Patient Command is an early stage company that is developing an electronic personal health record (PHR) for consumers' use on the Internet. Patient Command uses the model of a health record bank.

Consumers obtain copies of their medical records by making requests to providers under HIPAA (45 CFR §164.524). Whether providers furnish copies in electronic form or on paper, the copies can be input to Patient Command's system, which has proprietary features that can enhance the quality of information compiled in consumers' PHRs. Indeed, it is possible that consumers' Patient Command PHRs will be more accurate than the source documents from which they are assembled.

Because Patient Command is a health record bank, consumers own their PHRs and control them within a framework of rights and responsibilities. Two fundamental elements of the health record bank model are consumer control and consumer trust. Both these elements in turn rest on comprehensive security and privacy. Patient Command's system is built from the ground up to incorporate privacy and security comprehensively.

Patient Command's success in the marketplace will depend on its having security and privacy protections that are practical, effective, enforceable, and understandable to consumers. For these reasons, HIPAA's security and privacy rules are not suited to our planned operations, nor, we believe, to the operations of other entities offering PHRs to the public using the health record banking model.

HIPAA Privacy and Security: Complex, Costly, Ineffective

HIPAA's privacy and security rules are rightly criticized for being so complex that people do not understand them and therefore cannot apply them uniformly, much less effectively. Most consumers have little or no idea what the HIPAA regulations say or mean. Consumers only see impenetrable notices of privacy practices, endure apparently needless (and often seemingly endless) HIPAA forms that they must sign, and face regulatory obstacles when they want to transfer their medical records from one doctor or hospital to another for treatment purposes.

HIPAA's privacy and security regulations are so complex that, for practical purposes, the federal government is not enforcing them. (See Appendix, Press Report 1.) There is ever-more widespread recognition that the federal government has bungled HIPAA's implementation. For example, the Chairman of Microsoft, Bill Gates, recently called on the government to replace HIPAA with comprehensive privacy legislation that would be effective. (See Appendix, Press Report 2.)

These press articles are a tiny sample of published criticisms of HIPAA's privacy and security regulations. A fair sampling of the literature would lead the CPS Workgroup to conclude that, indeed, HIPAA is hardly the answer to hopes for a workable privacy regime for health records.

Patient Command believes that the Workgroup should conduct just such a survey of the popular and academic literature about HIPAA before it considers recommending an expanded reach for HIPAA's privacy and security rules. A fair review of that literature – of which the Appendix to these comments is a tiny sample – should lead the Workgroup to abandon any notion of adopting HIPAA's rules for health information exchanges. Instead, HIPAA's rules should be restricted to covered entities and their business associates, as is now the case, until Congress can mandate a path to replacing HIPAA's rules with more sensible, less complex regulations that can, for practical purposes, actually be enforced.

HIPAA's complexity of course also makes compliance with its rules needlessly expensive. As the Workgroup contemplates security and privacy aspects of electronic health data exchanges, please keep in mind that system costs will be passed on to consumers and to doctors and hospitals. Cost-effectiveness – a set of criteria by which HIPAA does poorly or worse – should be a touchstone for the Workgroup. Viewed in that light, HIPAA's privacy and security regulations are not a good choice for governing electronic health data exchanges.

Enabling Consumer Choice: Present Laws Protecting Security and Privacy of Medical Records

Existing federal and state laws besides HIPAA protect the security and privacy of consumers' health records. This is certainly true for health records deposited in PHR systems that use the health record banking model.

For example, Patient Command will offer its services to consumers through a member agreement. Our representation about our services as described on our web site, in our literature, and in our standard contracts with consumers will all be subject to existing consumer protection laws. These laws are enforced at the federal level by, among other agencies, the Federal Trade Commission. They are also enforced by a variety of state consumer protection agencies.

This existing regime of federal and state consumer protections is far more comprehensive, and far more suited as a practical matter to govern the operation of health record banks, than the HIPAA rules. A Procrustean attempt to adapt the HIPAA rules – designed, after all, for HIPAA "covered entities" and their business associates – to consumer health record banking would be an arduous, contentious process, and it would be doomed from the start. HIPAA rules simply are inferior to the laws that now apply.

How is this so?

First, the FTC and state consumer protection agencies know how to run effective enforcement regimes. This is in stark contrast to HIPAA. Second, existing consumer protection enforcement is comprehensible to many consumers, something that cannot be said of HIPAA. Third, attempting to overlay HIPAA rules on existing federal and state consumer protection laws that will be enormously confounding. As applird to health record banks, a HIPAA overlay would create substantial legal issues involving preemption, comity, and primary jurisdiction. Fourth and most important, applying HIPAA privacy and security rules to the health record banking model would be likely actually to constrain consumer choice. It would have this unfortunate effect because HIPAA privacy and security rules are, as noted, overly complex. Health record banks and the customers they serve therefore would face unnecessary regulatory obstacles in acquiring, storing, and moving consumer information, and in making that information useful, according to the wide variety of preferences that consumers will want to exercise.

Conclusion

For all these reasons, Patient Command urges the Workgroup to become familiar with existing federal and state consumer protection laws that apply to, among others, health record banks. We believe you will conclude that the existing legal framework is far better suited to establishing an enforceable, sustainable privacy regime than an extension of HIPAA to health record banking.

Respectfully submitted,

/s/ Richard D. Marks

Richard D. Marks
President
Patient Command, Inc.
6004 Balsam Drive
McLean, Virginia 22101
(703) 536-5525
richardmarks@earthlink.net

Appendix

Press Report 1

Medical Privacy Law Nets No Fines

Lax Enforcement Puts Patients' Files At Risk, Critics Say

By Rob Stein
Washington Post Staff Writer
Monday, June 5, 2006; A01

In the three years since Americans gained federal protection for their private medical information, the Bush administration has received thousands of complaints alleging violations but has not imposed a single civil fine and has prosecuted just two criminal cases.

Of the 19,420 grievances lodged so far, the most common allegations have been that personal medical details were wrongly revealed, information was poorly protected, more details were disclosed than necessary, proper authorization was not obtained or patients were frustrated getting their own records.

The government has "closed" more than 73 percent of the cases -- more than 14,000 -- either ruling that there was no violation, or allowing health plans, hospitals, doctors' offices or other entities simply to promise to fix whatever they had done wrong, escaping any penalty.

"Our first approach to dealing with any complaint is to work for voluntary compliance. So far it's worked out pretty well," said Winston Wilkinson, who heads the Department of Health and Human Services' Office of Civil Rights, which is in charge of enforcing the law.

While praised by hospitals, insurance plans and doctors, the approach has drawn strong criticism from privacy advocates and some health industry analysts. They say the administration's decision not to enforce the law more aggressively has not safeguarded sensitive medical records and has made providers and insurers complacent about complying.

"The law was put in place to give people some confidence that when they talk to their doctor or file a claim with their insurance company, that information isn't going to be used against them," said Janlori Goldman, a health-care privacy expert at Columbia University. "They have done almost nothing to enforce the law or make sure people are taking it seriously. I think we're dangerously close to having a law that is essentially meaningless."

The debate has intensified amid a government push to computerize medical records to improve the efficiency and quality of health care. Privacy advocates say large, centralized electronic databases will be especially vulnerable to invasions, making it even more crucial that existing safeguards be enforced.

The highly touted Health Insurance Portability and Accountability Act -- known as HIPAA -- guaranteed for the first time beginning in 2003 that medical information be protected by a uniform national standard instead of a hodgepodge of state laws.

The law gave the job of enforcement to HHS, including the authority to impose fines of $100 for each civil violation, up to a maximum of $25,000. HHS can also refer possible criminal violations to the Justice Department, which could seek penalties of up to $250,000 in fines and 10 years in jail.

Wilkinson would not discuss any specific complaints but said his office has "been able to work out the problems . . . by going in and doing technical assistance and education to resolve the situation. We try to exhaust that before making a finding of a technical violation and moving to the enforcement stage. We've been able to do that."

About 5,000 cases remain open, and some could result in fines, Wilkinson said. "There might be a need to use a penalty. We don't know that at this stage."

His office has referred at least 309 possible criminal violations to the Justice Department. Officials there would not comment on the status of those cases other than to say they would have been sent to offices of U.S. attorneys or the FBI for investigation. Two cases have resulted in criminal charges: A Seattle man was sentenced to 16 months in prison in 2004 for stealing credit card information from a cancer patient, and a Texas woman was convicted in March of selling an FBI agent's medical records.

Representatives of hospitals, insurance companies, health plans and doctors praised the administration's emphasis on voluntary compliance, saying it is the right tack, especially because the rules are complicated and relatively new.

"It has been an opportunity for hospitals to understand better what their requirements are and what they need to do to come into compliance," said Lawrence Hughes of the American Hospital Association.

"We're more used to the government coming down with a heavy hand where it's unnecessary," said Larry S. Fields, president of the American Academy of Family Physicians. "I applaud HHS for taking this route."

But privacy advocates say the lack of civil fines has sent a clear message that health organizations have little to fear if they violate HIPAA.

"It's not being enforced very vigorously," said William R. Braithwaite of the eHealth Initiative and Foundation, an independent, nonprofit research and advocacy organization

based in Washington. "No one is afraid of being fined or getting bad publicity. . . . As long as they respond, they essentially get amnesty."

The approach has made health-care organizations complacent about protecting records, several health-care consultants said. A recent survey by the American Health Information Management Association found that hospitals and other providers are still not fully complying, and that the level of compliance is falling.

"They are saying, 'HHS really isn't doing anything, so why should I worry?' " said Chris Apgar of Apgar & Associates in Portland, Ore., a health-care industry consultant.

Goldman and others also questioned why the government is not conducting more independent audits of compliance in addition to investigating complaints.

"It's like when you're driving a car," said consultant Gary Christoph of Teradata Government Systems of Dayton, Ohio. "If you are speeding down the highway and no one is watching, you're much more likely to speed. The problem with voluntary compliance is, it doesn't seem to be motivating people to comply."

Wilkinson's office has conducted just a "handful" of compliance reviews, an HHS spokesman said, and completed one -- a case involving a radiology center that was dumping old files of patients into an unsecured trash bin. The center agreed to hire a company to dispose of records and no fine was levied, the spokesman said.

Wilkinson said the size of his staff limits its ability to do much more than respond to complaints.

"We've had challenges with our resources investigating complaints," he acknowledged, saying they are complaint-driven. Wilkinson added, "We've been successful with voluntary compliance, so there has not been a need to go out and look."

But other government regulators take a different approach, privacy advocates say.

"The Securities and Exchange Commission, the Federal Trade Commission -- they find significant and high-profile cases and send a message to industry about what is permitted and what isn't," said Peter Swire, an Ohio State University law professor who helped write the HIPAA regulations during the Clinton administration.

Goldman and other privacy advocates point to numerous reports of health information being made public without patients' consent -- the recent theft of millions of veterans' records that included some medical information, a California health plan that left personal information about patients posted on a public Web site for years, and a Florida hospice that sold software containing personal patient information to other hospices.

In the meantime, Goldman said, surveys continue to show that for fear that their medical information will be used against them, people avoid seeking treatment when they are

sick, pay for care out of pocket, or withhold important details about their health from their doctors.

"The law came about because there was a real problem with people having their privacy violated -- they lost jobs, they were embarrassed, they were stigmatized. People are afraid. The law was put in place so people wouldn't have to choose between their privacy and getting a job or going to the doctor," said Goldman, who also heads the Health Privacy Project, a Washington-based advocacy group. "That's still a huge problem."

Press Report 2

This story appeared on Network World at
http://www.networkworld.com/news/2007/030807-gates-calls-for-new-privacy.html

Gates calls for new privacy law

By Grant Gross, IDG News Service, 03/07/07

Microsoft Chairman Bill Gates asked the U.S. Congress to pass a comprehensive privacy law this year, allowing consumers to control how their personal information is used.

Gates repeated past Microsoft calls for a wide-ranging privacy law during a speech at advocacy group the Center for Democracy and Technology's (CDT) annual gala dinner Wednesday. A comprehensive privacy bill should allow consumers to control their personal data, should provide transparency about what their data is used for, and should notify them when their data has been compromised, Gates said.

Gates said he believes the U.S. can achieve a balance between privacy and protecting the country against terrorists and other criminals. But the balance will not be an easy one to create, Gates said.

While many U.S. residents would say they want as much privacy "as possible," law enforcement needs to be able to track criminals, Gates said. "These privacy issues are not as easy as you might think," he told the crowd.

Gates hinted that some privacy protections can go so far that they become annoying to consumers. He talked about the Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, which puts strict controls on the release of information. HIPAA too often asks patients to sign documents allowing the release of their medical records, he said.

HIPAA is evidence "we don't always get it right the first time," Gates said. "All I know is I keep signing those forms."

Another balance Congress needs to strike is between emerging technologies and privacy, said Senator Patrick Leahy, a Vermont Democrat and chairman of the Senate Judiciary Committee. Leahy also called on Congress to pass a privacy law.

But a privacy law cannot restrict new technologies, Leahy said. "I don't want to stop the technologies, I want to protect our privacy," he during the gala dinner. "I think we can do both."

The U.S. government spying on its residents is of particular concern, Leahy said. "I don't want to put a brake on technology, but on what my government can learn about me without letting me know," he said.

Leahy and Gates both said they have great hopes for the future of the Internet. "The Internet is a great tool," Leahy said. "Let's keep it a free tool."

The world is just at the beginning of the potential of the Internet coupled with personal computers, Gates added. Coming advances in storage, in bandwidth and in user-created content will make the Internet and even greater tool for democratic ideals, he said.

"We're just at the very beginning," he said.

The IDG News Service is a Network World affiliate.